NCIX
NATIONAL COUNTERINTELLIGENCE EXECUTIVE

Honorable Michelle Van Cleave
National Counterintelligence Executive
Remarks before the OPSEC Professionals Society
San Diego, California
May 24, 2005.

Ladies and Gentlemen:

I am delighted to be here with you in my beautiful home state, which, as our Governor says, is called "California." I had a rather magical childhood growing up here, not only because this is a great place to live but also because my father worked for the original "magic Kingdom" – Walt Disney productions. This meant free passes to Disneyland. It also meant access to Disney studios in Burbank, California, where among other things you could walk the streets of the original set of the TV series, Zorro. I have always found Zorro to be a great fictional character: the masked fighter of evils, righter of wrongs, and defender of the weak and oppressed. Yet during the day, he put on a careful act as Don Diego de la Vega, rich and pampered and somewhat of a sissy. This was an early example of really fine OPSEC.

My subject this morning is not the sign of the Z. Rather, it is U.S. counterintelligence, specifically the new National Counterintelligence Strategy, which President Bush recently approved, and its implications for you as security professionals.

Let me begin with a word of praise for each of you as individuals and for the OPSEC Professionals Society as well. NSDD 298 has stood the test of time, thanks in no small measure to the dedication of the people assembled here. Like CI, the OPSEC discipline is subtle and complex. Activity profiles and the conduct of normal business can work to the detriment of our intelligence and national security programs by revealing key indicators to our adversaries. Understanding this and what to do about it require a detailed focus on vulnerabilities in our national security activities, sophisticated knowledge of the capabilities of our foes and thorough understanding of available countermeasures.

The Bush Administration remains firmly committed to the implementation of OPSEC doctrine and methodology within the government and among the contractor community. And the Interagency OPSEC Support Staff and this society remain very important to that national effort.

As you know, last year Congress established a new structure for the US intelligence community. Just last week, President Bush presided over the swearing-in of the nation's first Director of National Intelligence, John Negroponte.

Director Negroponte has many challenges, chief among them, in the President's words, to make "sure that those whose duty it is to defend America have the information we need to make the right decisions …[and] that our intelligence agencies work as a single, unified enterprise."

This imperative to work as a single, unified enterprise is equally compelling for US counterintelligence.

Historically, the counterintelligence community has not been organized or structured to accomplish a national mission; rather, the various CI elements have grown out of individual department or agency needs. They are part of a loose confederation of independent organizations with narrower and varying responsibilities, jurisdictions and capabilities; and with no one in charge of the enterprise. Operations have tended to focus on individual cases and are conducted with little appreciation of the potential impact of a synergistic effort. Many previous CI deficiencies have been the result of this systemic failure in the architecture of our community.

To begin to remedy this situation and help bring strategic coherence to US CI, the Congress created the position of the National Counterintelligence Executive. The law directs that the NCIX shall serve as the head of counterintelligence for the US government, subject to the direction and control of the President and now the DNI. My responsibilities are to ensure the integration of all US CI activities, which covers a wide spectrum: collection, analysis, operations, and investigations, not to mention very different skill sets, cultures, and traditions. The purpose is to provide strategic direction to US CI, in order to enhance our ability to defeat foreign intelligence threats to our nation's security and vital interests.

Change is never easy; and under Director Negroponte's leadership, we in the US intelligence and counterintelligence community have much work to do. And we are committed to success. In this, we got some help from the WMD Commission, which the President charged, among other things, with reviewing the capabilities of the US intelligence community and recommending improvements. If you haven't had an opportunity to read their report, I commend it to you for its insightful critique and thoughtful ideas.

Indeed, it is an inherent quality of democratic government to seek ever better ways of meeting the responsibilities entrusted by the people.

Certainly that's how our Founding Fathers understood the job, as they gathered together in Philadelphia this very month over two centuries ago. The Articles of Confederation, which were written shortly before the British surrender at Yorktown, had established a Congress and a federal government, but one that was too weak to preserve a nation. The Constitutional Convention that first met on the morning of May 25, 1787 would set aside the Articles of Confederation, to develop through considered debate and compromise and providential inspiration the essential elements of a new Constitution for the United States. Within a mere four months, the document that has been our Nation's

bedrock was drafted, signed by 38 of 41 delegates present, and sent to the 13 states for ratification.

Under that enduring framework, generations of Americans have received both the blessings – and the responsibilities -- of freedom.

Within six decades, the number of states in the Union would double, with the admission of Florida and Texas just over the horizon, and America would look ever westward across a continent. How daunting a task it must have seemed to make one nation of diverse people scattered over such vast distances. And then there came nothing short of a technological miracle.

"What hath God wrought?" It was this very day in May in the year 1844 when Samuel Morse sent these words racing along a cable from the US Capitol to a railroad station in Baltimore, Maryland. Moments later, the answer came back: "What hath God wrought?" A fitting question, because from that first commercial telegraph line, our Nation – and the world – would be forever changed. Within 10 years some 20,000 miles of telegraph cable would crisscross the country, and the miracle of rapid communication over great distances would help enable America's expansion from the original colonies along the Eastern seaboard to the harbor town where we are meeting today.

Telephany and vastly more cables on land and undersea would follow -- as would the craft of those who aspired to tap them. And how to listen in on other things as well.

Which brings me to another interesting day in May some 45 years ago. On May 26, 1960, Ambassador Henry Cabot Lodge walked into the UN Security Council carrying a replica of the Great Seal of the United States. It had been a present from the Soviets to the US government, kept for many years on display at Spaso House, which as you know is the residence of the American ambassador in Moscow. This Great Seal was the same as the one that was crafted even before the Constitutional Convention and is now familiar to us all – but with one important difference. This bald eagle was bugged.

And it was quite a discovery. George Kennan's memoirs describe how the technician, "quivering with excitement … extracted from the shattered depths of the seal a small device, not much larger than a pencil . . . capable of being activated by some sort of electronic ray from outside the building. When not activated, it was almost impossible to detect. . . . It represented, for that day, a fantastically advanced bit of applied electronics," one of more than 100 other such devices that Lodge reported had been found in the U.S. embassies in Russia and other communist-bloc countries.

And despite the end of the Cold War, foreign interest in US secrets has not abated. Technological advances have enabled ever more capable collection devices. The cyber revolution has also made possible cyber espionage. And the old fashioned methods of human spies remain the most tried and true – and I would hasten to add, today there are more countries engaged in trying than ever before, with over a hundred nations and a few dozen suspected terrorist organizations targeting the US for intelligence collection.

In recent history, the United States has sustained stunning losses to foreign intelligence services, which penetrated through espionage and other means virtually every one of the most secret, highly guarded institutions of our national security apparatus. Some of this harm can be attributed to protective security vulnerabilities and failures, which I know the OPSEC discipline has taken to heart. But these losses also represent a strategic failure of our CI capabilities. Any one of these major compromises could have had devastating consequences in war. Thankfully, the Cold War ended, as President Reagan said, without either side firing a shot.

Today our Nation is at war, and the potential consequences of intelligence failure more immediate, placing in jeopardy US operations, deployed forces and our citizenry. And so I am seized with the need to do our job as though it were the morning after.

As my first boss in Washington, Jack Kemp, is fond of saying, freedom must be won anew by every generation. Our generation is no exception.

America faces substantial challenges to its security, freedom and prosperity. To meet them we must defeat global terrorism, counter weapons of mass destruction, ensure the security of the homeland, transform defense capabilities, foster cooperation with other global powers, and promote global economic growth. To state the obvious, our ability to meet these challenges is threatened by the intelligence activities of traditional and non-traditional foreign powers.

As an integral part of broader US national security policy and strategy, it is the job of US counterintelligence to discern and defeat the foreign intelligence threats to our nation, and to inform the protective security disciplines including the dynamic craft of OPSEC.

We now have, for the first time, a single document that sets forth the President's vision for US counterintelligence and its mission in support of America's national security. President Bush approved the National Counterintelligence Strategy on March 1st of this year. It is the first document issued by any Administration that directs the full scope of the Nation's efforts to counter the global foreign intelligence threats against the United States. It is modeled after the National Security Strategy of the United States. The Strategy, which is unclassified, is based on a classified threat assessment that lays out the ways in which foreign intelligence services are stealing U.S. national security secrets to support their war aims or terrorist objectives, or to undercut America's foreign policy or commerce, or to exploit what they learn of U.S. intelligence capabilities to hide their actions or mislead us. The strategic purpose of CI is to identify these threats and stop them.

For those who would like to read the Strategy, you may find a copy online on our website. For today, I would like to summarize its several parts, which are highly interrelated but also address discrete national security purposes and the people who are dedicated to those goals.

First the Strategy is addressed to those prosecuting the global war against terrorism.

In many parts of the world, including here at home, Al Qaida and other terrorist organizations employ classic intelligence methods to gather information, recruit sources, and run assets. They are also capable of engaging in sophisticated deceptive practices, not unlike traditional foreign powers, to deceive US decision-makers. Beyond this, terrorist groups draw strength from the support of state sponsors, which means that the intelligence services of those regimes can be key links in the global terrorist support network.

And so the Strategy directs that we ensure that the global war on terrorism is armor-plated with an effective CI strategy to identify and exploit offensive opportunities against terrorist networks, and to provide CI support to force protection and operations security in the field. Behind these straightforward objectives lie many intensive tasks, to bring analytic insight into the intelligence operations of terrorist groups and their sponsors, CI support to sensitive US operations, and a CI mindset to backstop the geopolitical imperatives of this global war.

The second part of the Strategy speaks directly to those who plan and carry out CI operations and investigations, whose job it is to discern, interdict and exploit the full range of foreign intelligence activities against us.

If you look back on the record of US counterintelligence, especially counter-espionage, you will see that most counterintelligence has been based on tolerating some level of loss – extremely grave loss in the case of some long-serving, well-placed spies – that, once discovered, triggers intensive investigations and prosecutions. This ability to react quickly and effectively will always be a vital core of CI. But US counterintelligence also needs to go on the offense.

To this end, the Strategy directs that US CI shift emphasis from a posture of reacting to a proactive strategy of seizing advantage. This is a sharp departure from past practices, but fully consistent with the President's strategy for the global war on terrorism. No longer will we simply rest on our ability to tolerate some level of loss before taking action. No longer will we cede the initiative to foreign intelligence services working on US soil to penetrate our government. The age-old wisdom that the best defense is a good offense is also true for counterintelligence.

What does it mean to go on the offense? Conceptually, there are two parts: First, a global CI assessment and engagement of adversary presence, capabilities and intentions. And second, a CI doctrine for attacking foreign intelligence services systematically via strategic CI operations.

The proactive approach to counterintelligence requires a generous dose of creativity to turn threat into opportunity. We don't want to sit back and discover, years

and years after the fact, that while we have investigated every reported security breach, spies have stolen our secrets or cyber thieves have exploited our networks. Instead, we need to think offensively.

We need to ask, what are the indicators that might give us early warning of intelligence operations against us? We need to ask, what can we do to discern and defeat such operations? Investigations are one among a suite of tools that the operational CI elements can employ; and there are others. And I look to the security offices within the government and industry – which is to say, to many of you -- to provide the knowledge, programs, and creative insights to engage the operational CI resources of the government to proactive ends.

Within the US, the proactive CI mission calls for a coordinated, community-wide effort of aggressive operational activity and analysis to obtain the intelligence necessary to neutralize the inevitable penetrations of our government. In order to do this, the operational and analytic focus of US CI must transform from a case-driven approach to a strategic assessment of adversary presence, capabilities and intentions, which in turn drives operations. This will also require looking beyond the customary targets of known intelligence officers to the larger population of diverse foreign visitors and others serving foreign intelligence purposes, who find our free and open society a rich playing field for the illicit collection of national security secrets and other valuable information that confers advantage.

This brings me to the third part of the Strategy, which addresses the stewards of our Nation's defense industrial base. It is the objective of US counterintelligence to help protect the vital technology secrets that are the bedrock of our strategic security.

America's national defense rests on its continuing technological superiority. The United States cannot maintain its dynamic technological superiority without a corresponding intelligence and counterintelligence superiority.

A national defense strategy based on transformation places a premium on the sensitive capabilities and technologies that give advantage. The single most effective strategy to defeat U.S. plans to ensure superiority through transformation is to capture those essential secrets, in order to incorporate them into adversary weapons systems and to develop countermeasures. Foreign militaries that acquire controlled U.S. technologies are able to leapfrog technological barriers that would otherwise slow or even prevent the production of more sophisticated weapons.

As you are all aware, espionage has long proven the most cost-effective means of defeating U.S. capabilities. We may spend billions of dollars to develop a given weapons system, the effectiveness of which rests on essential technological, operational or design secrets that give us advantage. If those essential secrets are stolen, both our investments and our advantage can be lost. The cost-benefit ratio of espionage is sharply in the adversary's favor.

The most successful espionage – the kind that goes undetected – is all the more effective, because what is not known cannot be remedied. And the risks are growing. The marvels of modern information technology and microelectronics have revolutionized espionage tradecraft, enabling the clandestine extraction of vast volumes of data in miniaturized storage media or across computer networks at the press of a "send" button.

The key to protecting America's qualitative defense advantage is to draw upon all of the tools of statecraft, national policy, law enforcement and public awareness to deny adversary acquisition of essential technology secrets. These things must be done in concert. That is a policy call. But CI needs to supply insights into the foreign intelligence threats against vital technologies, and options to counter those threats. That will require focused and creative collection activities, strategic analytic exploitation, and coordinated operational discipline. In this manner, CI can make a seminal contribution to the overall national technology protection effort.

The fourth part of the Strategy speaks to the collectors and analysts of intelligence and other information that must withstand the efforts of adversaries to manipulate our perceptions of reality. It reads: "It is the objective of US counterintelligence to safeguard the integrity of intelligence and to identify and defeat foreign denial, deception and covert influence operations."

Successful foreign penetrations both human and technical have netted foreign intelligence services an enormous amount of U.S. classified information, enabling debilitating countermeasures to U.S. intelligence collection and analysis. There is a market for stolen U.S. secrets, which can be sold or bartered to third party states or terrorist organizations that have their own uses for the information. The knowledge gained of U.S. intelligence sources and methods -- through spies, unauthorized disclosures, and even some authorized disclosures -- has aided in extensive concealment and denial programs that increase our uncertainty about foreign capabilities and intentions, and deception operations to mislead us.

As a result of sensitive knowledge gained about U.S. intelligence, many nations have learned how to deny and deceive the United States in order to present a false picture of reality. These foreign denial and deception practices may lead analysts to faulty judgments, when vital information has not been collected, or when deception distorts understanding. The danger is that useless or deceptive information – whether from human or technical collection -- may be integrated into U.S. intelligence and disseminated to policymakers, weapons designers, war-fighters and even the warning community as if it were true. It is the job of counterintelligence collection and analysis to protect and validate U.S. intelligence and to reveal otherwise unknown strengths and weaknesses and threats posed by U.S. adversaries.

The fifth part of the Strategy turns to US business and industry, which need a level playing field in the face of foreign competitors, some of whom have the active support of their governments. The concern is that, when it comes to commercially valuable financial and technical information, private American firms may find

themselves competing not just with other companies but on occasion against foreign intelligence services as well.

The protection of American strategic information and technology has long been an element of the nation's security, including the propriety commercial information that brings competitive advantage. Lead responsibility for that job of course falls to the private sector owners of that information and technology. But government also has a role to play. As a first and obvious step, government can provide information about the threat, to the extent that intelligence is available and can be confidently shared. But it is up to business and industry to decide what to do. There will always be some level of risk. Deciding how to manage that risk, in order to carry out operations effectively, is the real security challenge and the heart of the OPSEC discipline.

As everyone here knows full well, CI and security cannot be afterthoughts imposed on corporate R&D personnel, businessmen or mid-level managers. Heightened awareness, and intelligent security practices that protect the valuable secrets of the corporation, are the best guarantors of success against the foreign intelligence threat. While our principal focus must remain the terrorist threat, we will also enhance outreach to the private sector to increase awareness of the economic intelligence threat facing our Nation as a whole, through providing threat information, and educating especially the S&T community, to the variety of ways our adversaries acquire and steal information from us.

The sixth part of the Strategy addresses our national security policymakers.

A major responsibility of my office is to help ensure that the national security decision-making process is informed by counterintelligence insights.

The intelligence activities of adversaries or allies, competitors or partners, are a window into their respective interests, purposes and plans. For instance, our insights into the foreign intelligence activities of the other main centers of global power may confirm or otherwise shape prospects for cooperative action. Good CI analysis can help discover and connect the seemingly disconnected, to reveal patterns of activity and behavior heretofore unobserved. CI analysts are the ones who zero in on the things Yoggi Berra deemed “too coincidental to be a coincidence.”

My office is also charged with performing damage assessments of espionage cases, which also have insights to contribute to decision-makers. These include the direct impact of the damage on US intelligence and national security plans and programs, as well as the vulnerabilities revealed, and managerial, security and operational lessons learned.

In effect, under this Strategy counterintelligence will have a guest seat at the policy table, in order to present an array of strategic CI insights and operational options in foreign and defense policy for the President and his national security leadership team.

Finally, the Strategy directs that we build a national system – the institutions and processes -- capable of supporting and executing these objectives of US counterintelligence. And that work is underway, in concert with larger structural and procedural changes across our intelligence institutions. These include augmenting our strategic analytic capability, bringing coherence to budgeting and programming, and developing modalities for strategic operational planning that can reach across all the CI resources of the US government.

The conference planners have an ambitious agenda for you this week, which covers many fascinating and important topics. The OPSEC discipline is demanding, and the challenges you face often changing and complex. In this, you are not alone.

I am reminded of what President Bush said in his second Inaugural Address. "From the perspective of a single day, the issues and questions before our country are many. From the viewpoint of centuries, the questions that come to us are narrowed and few. Did our generation advance the cause of freedom? And did our character bring credit to that cause?"

I am grateful to be here with you this morning, and to work with you, to advance our common goal: that in the future, we might be able to answer these two compelling questions with a confidant and humble, Yes.